

SEC300

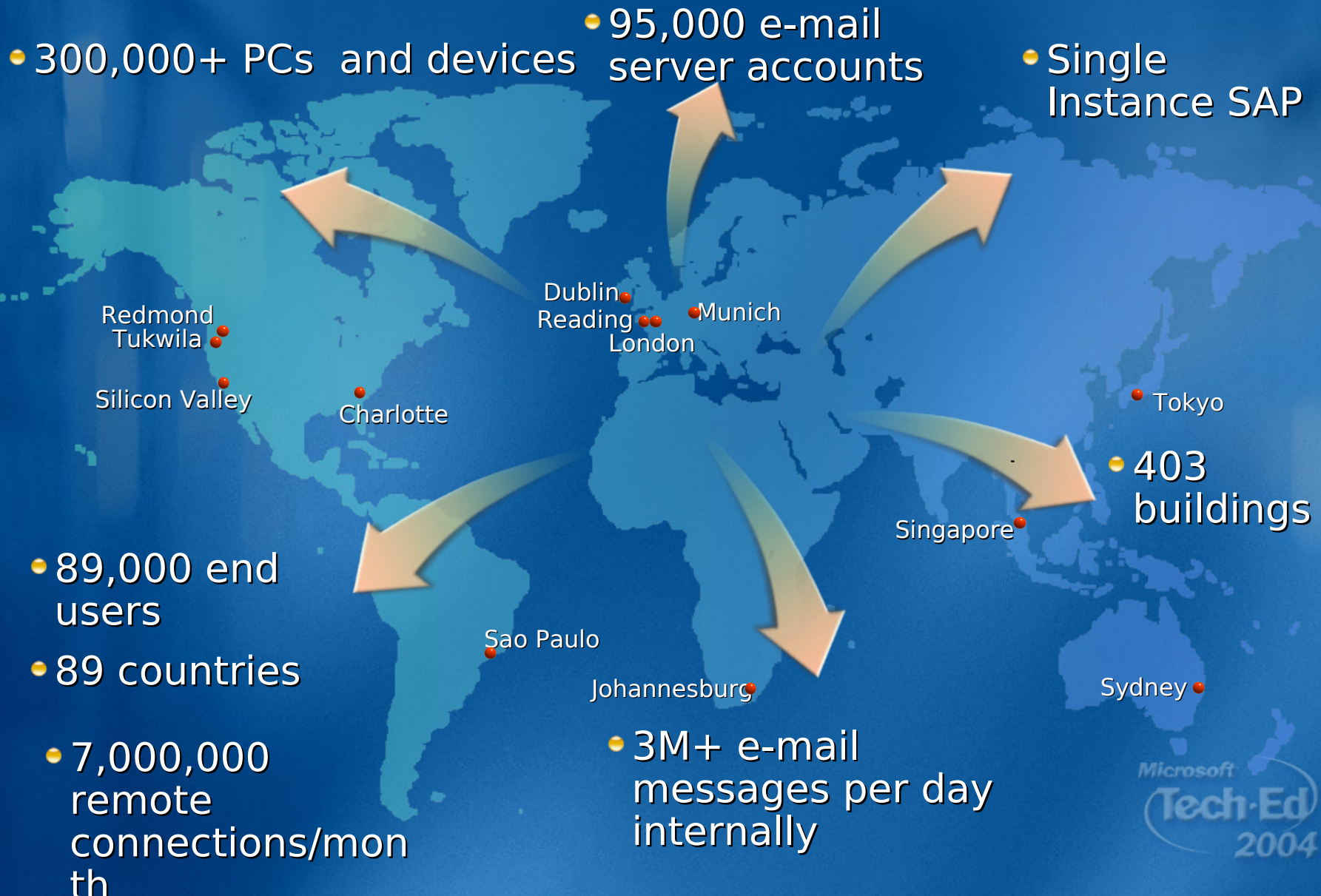
Securing Microsoft: How Microsoft Does IT

**Michael Sharp
Director, IT Security
Microsoft**

Agenda

- **Microsoft environment**
- **Security strategy**
 - **Mission and vision**
 - **Security principles**
 - **Risk-based decision model**
 - **Tactical prioritization**
- **Representative risks and tactics**
- **Organization chart**

Microsoft IT Data



Microsoft Security Environment

- **Environment**

- More than 300,000 network-joined devices
- 30,000 business partners with connectivity needs
- Frequent target of attack

- **Challenges**

- Culture based on autonomy and agility
- Large population of mobile clients
- Unique business requirements to support software development
- Running the business on N+1 platform as "first and best" customer

Security Strategy

**Corporate
Security Mission
and Vision**

**Security
Operating
Principles**

Risk-Based Decision Model

Tactical Prioritization

Mission

Prevent malicious or unauthorized use that results in the loss of Microsoft intellectual property or productivity by systematically assessing, communicating, and mitigating risks to digital assets



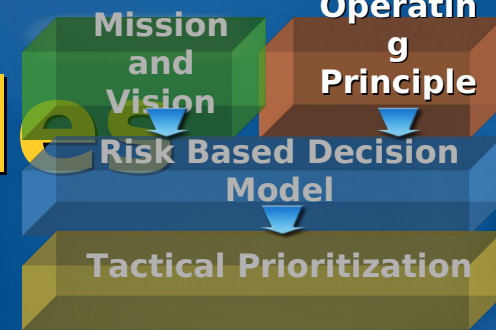
Vision



An IT environment comprised of services, applications, and infrastructure that implicitly provides availability, privacy, and security to any client

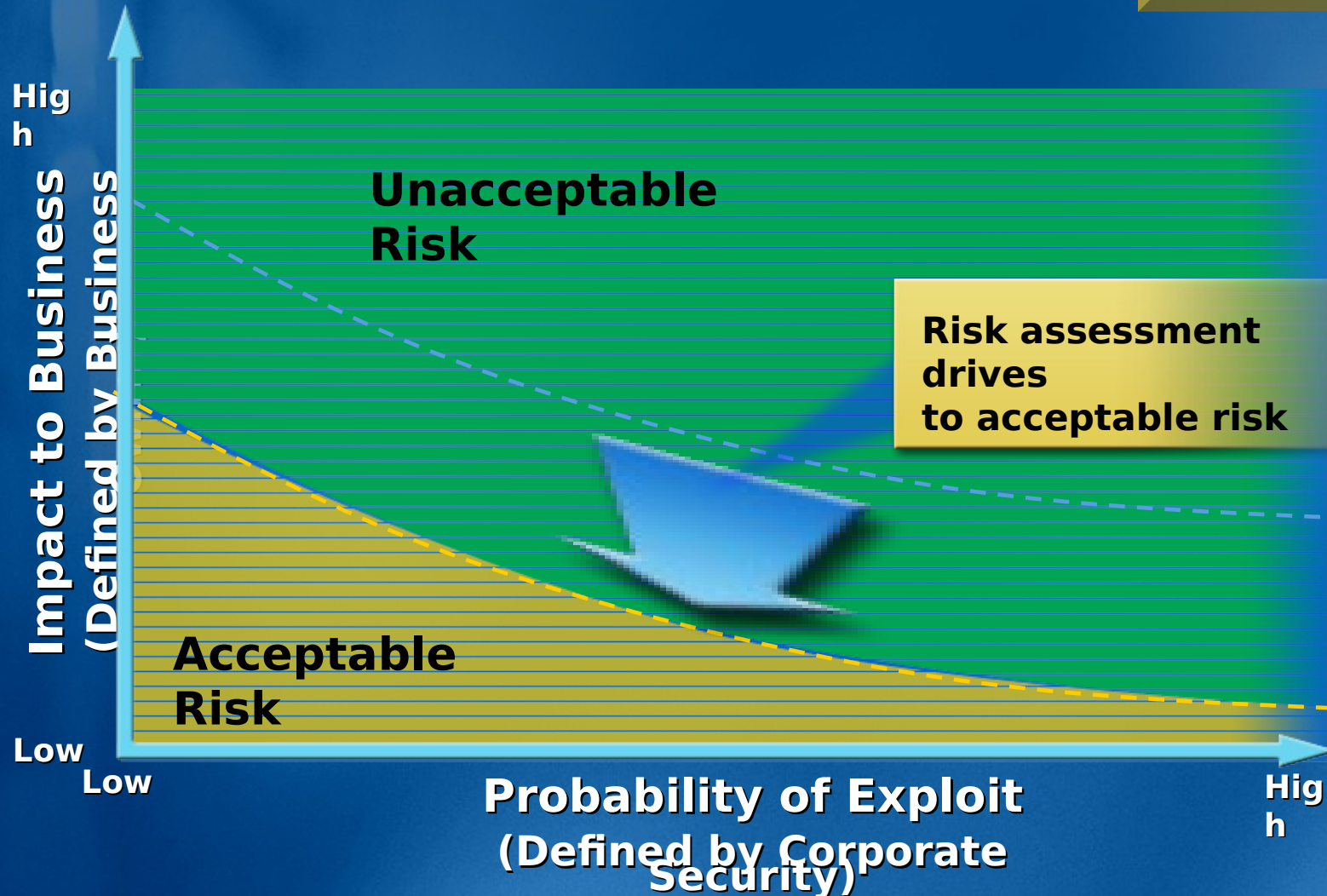
- **Five Trustworthy Assurances**
 - **My identity is not compromised**
 - **Resources are secure and available**
 - **Data and communications are private**
 - **Roles and accountability are clearly defined**
 - **There is a timely response to risks and threats**

Operating Principles

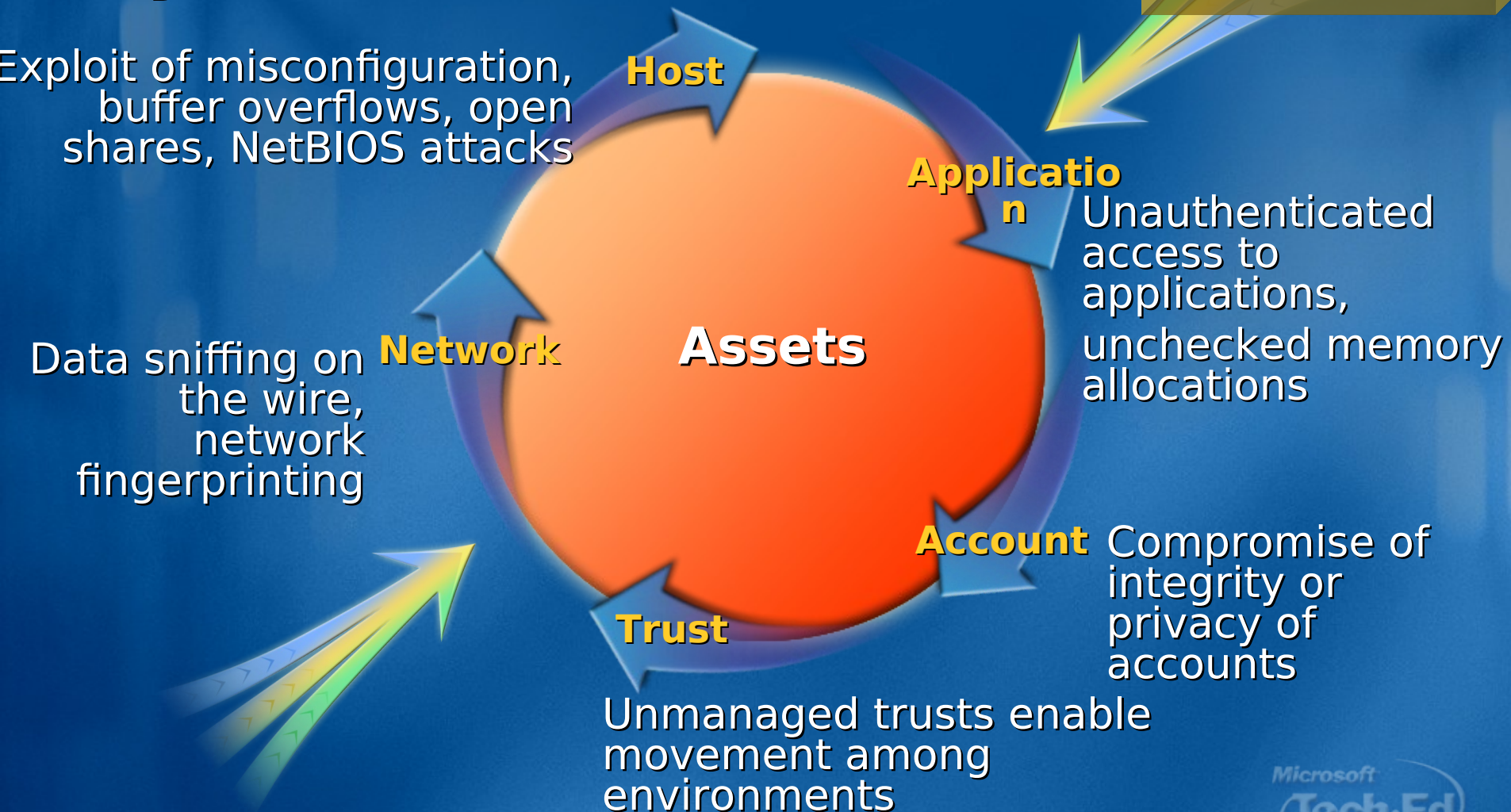
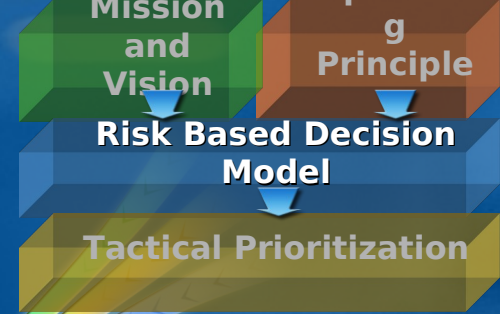


- **Management commitment**
 - Manage risk according to business objectives
 - Define organizational roles and responsibilities
- **Users and data**
 - Manage to practice of least privilege
 - Strictly enforce privacy and privacy rules
- **Application and system development**
 - Build security into development life cycle
 - Layered defense and reduced attack surface
- **Operations and maintenance**

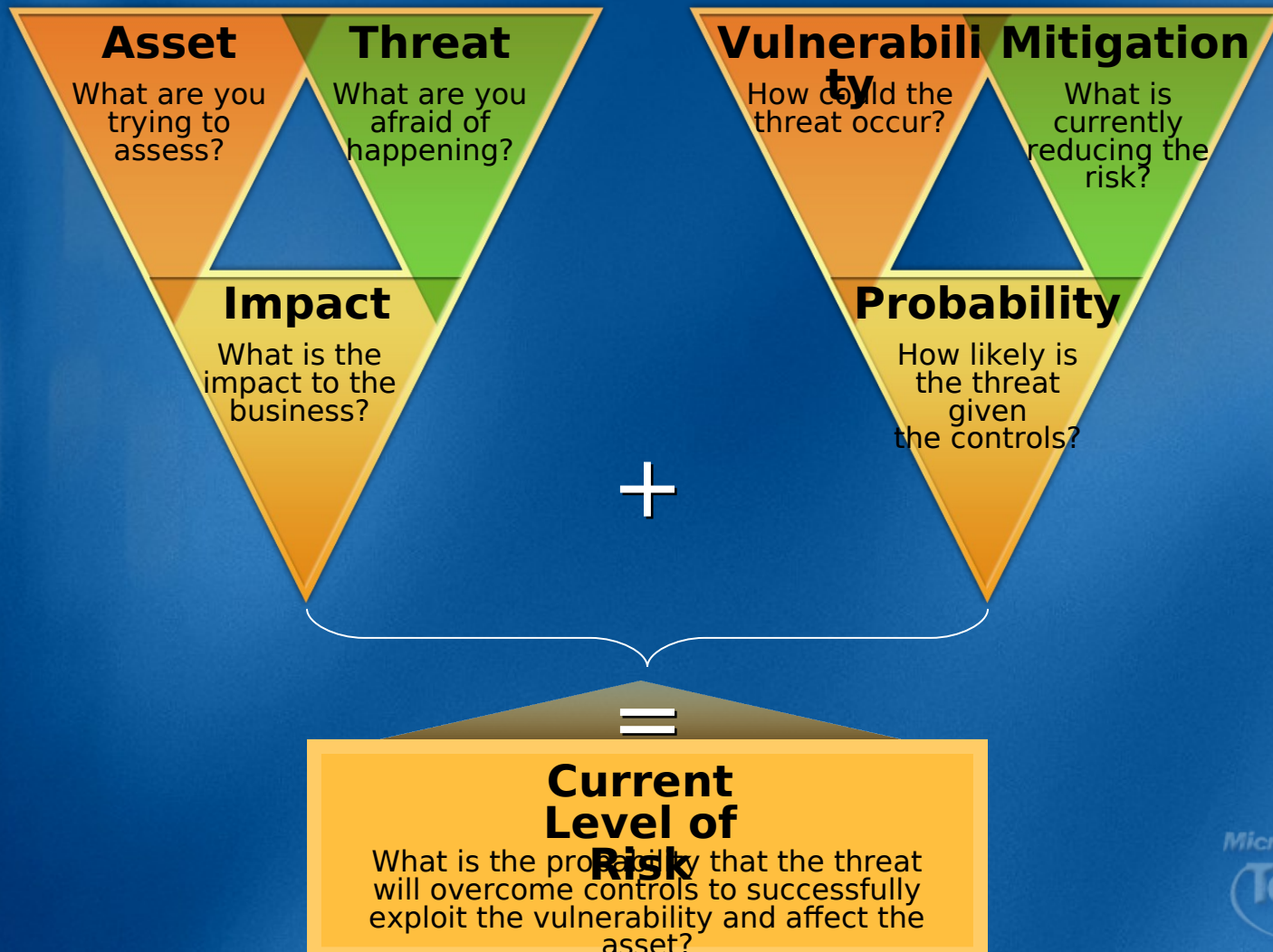
Enterprise Risk Model



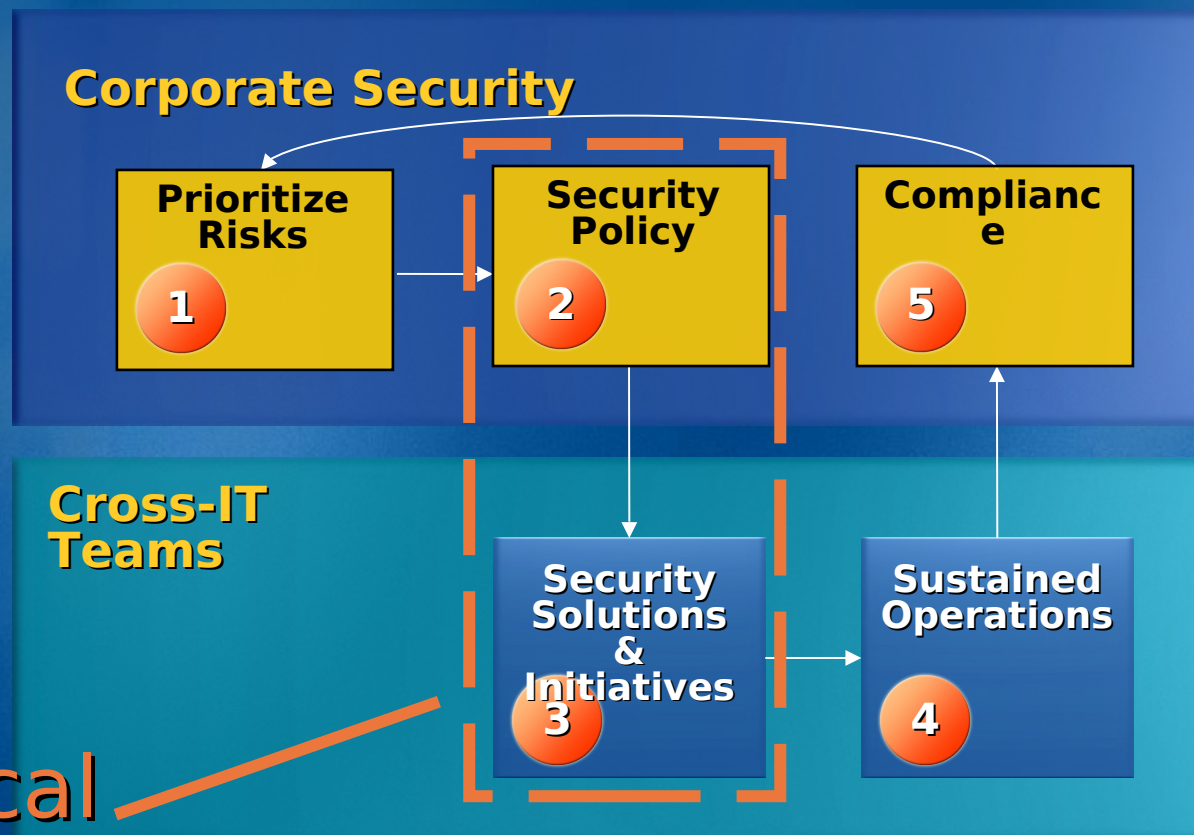
Risk Analysis By Asset Class



Components Of Risk Assessment

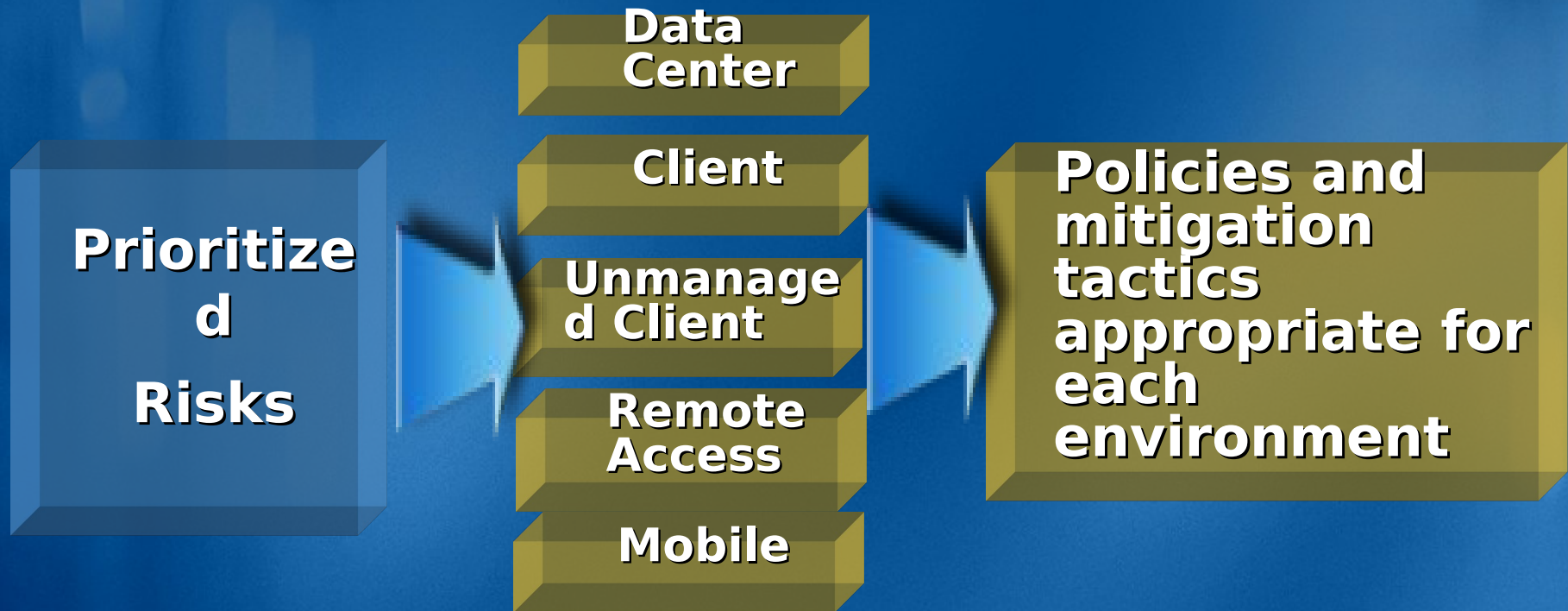


Risk Management Process And Roles



Tactical
Prioritization

Tactical Prioritization By Environment



Representative Risks And Tactics

Enterprise Risks

Unpatched Devices

Unmanaged Devices

Remote and Mobile Users

Single-Factor Authentication

Focus Controls Across Key Assets

Embody
Trustworthy
Computing

Tactical Solutions

Secure Environmental Remediation

Network Segmentation Through IPSec

Secure Remote User

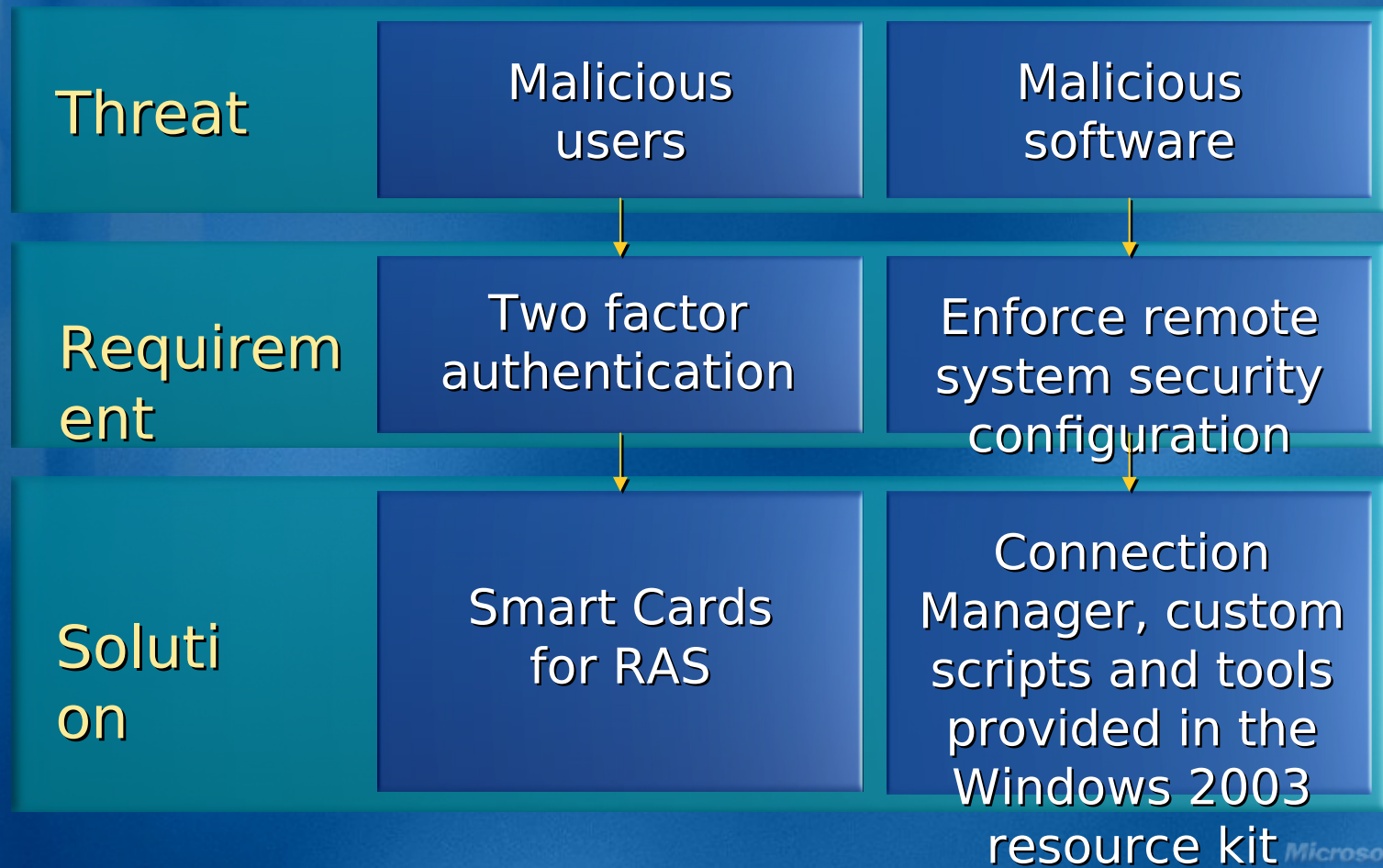
Two-Factor for Remote Access and Administrators

Managed Source Initiatives

Network Segmentation: Security Requirements And Goals

- **Mitigate risk posed to IT-managed computers by implementing a solution to:**
 - **Provide the capability to control access to all IT-managed computers on CorpNet at the network level**
 - **Define an IT-managed computer population**
 - **Segment IT-managed computers from unmanaged computers (i.e. network-level boundary)**
 - **Allow IT-managed computers to have the ability to restrict network level access to a subset of IT-managed computers if required**
- **Network Segmentation Goals**
 - **Prevent unmanaged computers from initiating connections to IT-managed computers**
 - **IPsec is the only technology available now that**

Remote Access Security



Wireless Security

Overview

- 802.1x + EAP/TLS for authentication
- Session WEP keys for encryption
- Issue user & machine certificates from self-hosted Microsoft PKI
- Certificate to user mapping via the Active Directory
- Prohibited the use of non-IT managed access points by policy, with enforcement through scanning for rogue access points

Secure Messaging

- **Non-Repudiation & Encryption**
 - **S/MIME**
- **Information Protection**
 - **Information Rights Management**

Corporate Security Group Organization

Corporate Security Group



For More Information

- Additional content about Microsoft IT deployments and best practices can be found on <http://www.microsoft.com>
- Microsoft TechNet <http://www.microsoft.com/technet/itshowcase>
- Microsoft Case Study Resources [http://www.microsoft.com/resources/
casestudies](http://www.microsoft.com/resources/casestudies)
- E-mail IT Showcase

Session Evaluation

Please fill out a session evaluation on CommNet

Q1: Overall satisfaction with the session

Q2: Usefulness of the information

Q3: Presenter's knowledge of the subject

Q4: Presenter's presentation skills

Q5: Effectiveness of the presentation

Microsoft[®]

Your potential. Our passion.[™]

© 2004 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.